Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1. (original) A method for encrypting information using encryption keys, wherein each key encrypts a portion of information of a predetermined block length, the method comprising using a first key to encrypt a first portion of a message;

adding at least one bit of information to the encrypted first portion of the message;

using a second key to encrypt a second portion of the message wherein the second portion overlaps with the first portion and also includes the added one or more bits of information.

2. (new) A method for encrypting information in a message that can be authenticated, the method comprising:

adding a first authentication block to the information to be encrypted to form a concatenated field;

logically subdividing the concatenated field into predetermined block lengths, including a residual field when the concatenated field is not sized as an even multiple of the predetermined block length;

encrypting the subdivided fields using a key to form cipher blocks;

designating one of the cipher blocks as a designated cipher block, the other cipher blocks being nondesignated cipher blocks;

subdividing the designated cipher block into a first portion and a second portion, such that a combined length of the second portion and the residual field and a second authentication block is the predetermined block length;

encrypting the second portion and the residual portion together with the second authentication block using the key to form a cipher residual block; and

providing at least the first portion of the designated cipher block, the nondesignated cipher blocks and the cipher residual block as the message such that the message can be authenticated by decryption of a valid authentication block of either the first authentication block or the second authentication block.

3. (new) The method of claim 2, wherein the second authentication block comprises one or more bits and the second portion is less than 128 bits.

4. (new) The method of claim 2, wherein the second authentication block comprises one or more bits forming a null value.

5. (new) A method for encrypting and decrypting information in a message that can be authenticated, the method comprising:

adding a first authentication block to the information to be encrypted to form a concatenated field;

logically subdividing the concatenated field into predetermined block lengths, including a residual field when the concatenated field is not sized as an even multiple of the predetermined block length;

encrypting the subdivided fields using a key to form cipher blocks;

designating one of the cipher blocks as a designated cipher block, the other cipher blocks being nondesignated cipher blocks;

subdividing the designated cipher block into a first portion and a second portion, such that a combined length of the second portion and the residual field and a second authentication block is the predetermined block length;

encrypting the second portion and the residual portion together with the second authentication block using the key to form a cipher residual block; and

providing at least the first portion of the designated cipher block, the nondesignated cipher blocks and the cipher residual block as the message such that the message

can be authenticated by decryption of a valid authentication block of either the first authentication block or the second authentication block;

decrypting at least the cipher residual block to obtain a representation of the second authentication block;

a1

authenticating the message by comparing the representation of the second authentication block to an expected value for the second authentication block;

decrypting the cipher blocks to obtain at least a representation of the first authentication block; and

further authenticating the message by comparing the representation of the first authentication block to an expected value for the first authentication block.